

08/28/00

JCG65 U.S. PRO

Please type a plus sign (+) inside this box → **+**

Approved for use through 09/30/2000. OMB 0851-0032
 Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
 Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UTILITY PATENT APPLICATION TRANSMITTAL (Only for new nonprovisional applications under 37 C.F.R. § 1.53(b))	Attorney Docket No. 017.38726X00
	First Inventor or Application Identifier Piotr COFTA
	Title See 1 in Addendum
	Express Mail Label No. _____

APPLICATION ELEMENTS See MPEP chapter 600 concerning utility patent application contents.	ADDRESS TO: Assistant Commissioner for Patents Box Patent Application Washington, DC 20231
1. <input checked="" type="checkbox"/> * Fee Transmittal Form (e.g., PTO/SB/17) (Submit an original and a duplicate for fee processing)	5. <input type="checkbox"/> Microfiche Computer Program (Appendix)
2. <input checked="" type="checkbox"/> Specification (preferred arrangement set forth below)	6. Nucleotide and/or Amino Acid Sequence Submission (if applicable, all necessary)
[Total Pages 18] - Descriptive title of the Invention - Cross References to Related Applications - Statement Regarding Fed sponsored R & D - Reference to Microfiche Appendix - Background of the Invention - Brief Summary of the Invention - Brief Description of the Drawings (if filed) - Detailed Description - Claim(s)	a. <input type="checkbox"/> Computer Readable Copy b. <input type="checkbox"/> Paper Copy (identical to computer copy) c. <input type="checkbox"/> Statement verifying identity of above copies
3. <input checked="" type="checkbox"/> Drawing(s) (35 U.S.C. 113) [Total Sheets 6]	ACCOMPANYING APPLICATION PARTS
4. Oath or Declaration [Total Pages 2]	7. <input checked="" type="checkbox"/> Assignment Papers (cover sheet & document(s))
a. <input checked="" type="checkbox"/> Newly executed (original or copy) b. <input type="checkbox"/> Copy from a prior application (37 C.F.R. § 1.63(d)) (for continuation/divisional with Box 16 completed)	8. <input type="checkbox"/> 37 C.F.R. § 3.73(b) Statement of Attorney (when there is an assignee)
i. <input type="checkbox"/> DELETION OF INVENTOR(S) Signed statement attached deleting inventor(s) named in the prior application, see 37 C.F.R. §§ 1.63(d)(2) and 1.33(b).	9. <input type="checkbox"/> English Translation Document (if applicable)
* NOTE FOR ITEMS 1 & 13 IN ORDER TO BE ENTITLED TO PAY SMALL ENTITY FEES, A SMALL ENTITY STATEMENT IS REQUIRED (37 C.F.R. § 1.27), EXCEPT IF ONE FILED IN A PRIOR APPLICATION IS RELIED UPON (37 C.F.R. § 1.28).	10. <input checked="" type="checkbox"/> Information Disclosure Statement (IDS) (PTO-1449) <input checked="" type="checkbox"/> Copies of IDS Citations
	11. <input type="checkbox"/> Preliminary Amendment
	12. <input checked="" type="checkbox"/> Return Receipt Postcard (MPEP 503) (Should be specifically itemized)
	13. <input type="checkbox"/> Small Entity Statement(s) <input type="checkbox"/> Statement filed in prior application Status still proper and desired
	14. <input type="checkbox"/> Certified Copy of Priority Document(s) (if foreign priority is claimed)
	15. <input checked="" type="checkbox"/> Other: Credit Card Payment Form

16. If a CONTINUING APPLICATION, check appropriate box, and supply the requisite information below and in a preliminary amendment:

☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No. _____ / _____

Prior application information: Examiner _____ Group / Art Unit: _____

For CONTINUATION or DIVISIONAL APPS only: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 4b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

17. CORRESPONDENCE ADDRESS

☒ Customer Number or Bar Code Label **020457** or ☐ Correspondence address below

(Insert Customer No. or Attach bar code label here)

Name			
Address			
City	State	Zip Code	
Country	Telephone	Fax	

Name (Print/Type)	David C. Oren	Registration No. (Attorney/Agent)	38,694
Signature		Date	8/28/00

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231.

Variable	Unit	Mean	Std. Dev.	Minimum	Maximum
Age	Years	35.2	12.5	20	65
Gender	Male/Female	0.45	0.50	0	1
Education	Years	12.8	2.1	8	16
Income	Dollars	45,000	15,000	20,000	80,000
Health	Good/Bad	0.60	0.49	0	1
Marital Status	Married/Single	0.75	0.43	0	1
Occupation	Professional/Service	0.55	0.50	0	1
Religion	Protestant/Catholic	0.40	0.50	0	1
Political Party	Democrat/Republican	0.50	0.50	0	1
Region	North/South	0.50	0.50	0	1
Urban/Rural	Urban/Rural	0.60	0.49	0	1
Home Ownership	Own/Rent	0.70	0.46	0	1
Vehicle Ownership	Own/Rent	0.80	0.40	0	1
Life Satisfaction	1-5	3.2	1.0	1	5
Health Satisfaction	1-5	3.5	1.0	1	5
Income Satisfaction	1-5	3.0	1.0	1	5
Marital Satisfaction	1-5	3.8	1.0	1	5
Occupational Satisfaction	1-5	3.3	1.0	1	5
Religious Satisfaction	1-5	3.6	1.0	1	5
Political Satisfaction	1-5	3.4	1.0	1	5
Regional Satisfaction	1-5	3.1	1.0	1	5
Urban/Rural Satisfaction	1-5	3.7	1.0	1	5
Home Ownership Satisfaction	1-5	3.9	1.0	1	5
Vehicle Ownership Satisfaction	1-5	4.0	1.0	1	5

- 117 | Page

017.38726X00
NC29782

UNITED STATES PATENT APPLICATION FOR:

**METHOD AND TOKEN FOR AUTHENTICATING A
CONTROL POINT**

Inventor:

PIOTR COFTA

Prepared by:

Antonelli, Terry, Stout & Kraus, LLP
1300 North Seventeenth Street, Suite 1800
Arlington, Virginia 22209
Tel: 703/312-6600
Fax: 703/312-6666

METHOD AND TOKEN FOR AUTHENTICATING A CONTROL POINT

FIELD OF THE INVENTION

The present invention generally relates to a method and apparatus for authenticating an action. More particularly, the present invention relates to a method and token for authenticating a control point in a transaction or action.

DESCRIPTION OF RELATED ART

Financial transaction such as payment at a point of sale (POS) or the dispensing of monies at an ATM machine often include authorization of the user or purchaser by the entity providing the service, payment or object desired. The user or purchaser must often present identification for the authentication such as a card (e.g. a credit card or debit card) or a badge in order for the entity to authorize a particular action. The entity (e.g., merchant) may then verify the identity of the user through information that is then conveyed by the card, badge or other structure presented by the user. For example, a purchaser may provide a credit or debit card to a merchant who runs it through a card scanner to read out financial identification (ID) associated with the card. The financial ID and the cost of the goods or services may be forwarded over a telephone network (such as the public switched telephone network) to the bank or other entity providing the credit for the credit card or maintaining the money associated with the debit card. The bank verifies that there is

sufficient credit or debt capacity for the transaction and forwards verification to the merchant. The consumer then is typically asked to sign a receipt for the purchase and the transaction is thereby completed and the goods or services are conveyed to the consumer. However, in these transactions, the user or purchaser must trust the entity that he is presenting his identification card or badge. The entity to whom he presents his identification may be a fraudulent entity and may steal vital data or monies from the user.

Under current methods, the user or purchaser is unable to verify the authenticity of the entity other than observing the brand name, label or name of the entity. Any uncommon occurrence such as a malfunction at the entity makes the user feel uncomfortable.

Secure electronic transactions (SET) have recently been used for secure credit card payments over the Internet. In a remote payment SET, both the purchaser and the merchant may entrust the same organization to perform an off-line verification process. This off-line verification process may be in the form of cryptographic data exchange between the purchaser and the merchant. However, secure electronic transactions do not address other aspects of the payment and assume that the purchaser is satisfied with the off-line authentication of the digital certificate that is presented by the merchant. It is desirable to obtain further authentication of merchants.

SUMMARY OF THE INVENTION

A method is provided for authenticating (or verifying) an action (e.g. financial action, access control, ticketing, and toll collecting) between a control point and a user.

The method may involve presenting a token to the control point and authenticating the control point using the token.

The authentication may occur on-line between the token and a token issuer that issued the token to the user.

The token may be a mobile communication device that communicates with the token issuer using a wireless communication path. The token may also communicate with the token issuer using a communication network of the control point. The control point may also authorize the action based on information provided by the token.

A token may be provided for authenticating a control point. The token may include a communication portion that obtains information regarding the control point and that communicates with an external entity (e.g., a token issuer) to authenticate the control point based on the information. A user interface portion may be coupled to the communication portion to indicate a result of the authentication to a user.

Other objects, advantages and salient features of the invention will become apparent from the following detailed description taken in conjunction with the annexed drawings, which disclose preferred embodiments of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention will be described with reference to the following drawings in which like reference numerals refer to like elements and wherein:

Figure 1 is a block diagram of entities involved in a financial transaction;

Figure 2 is a flow chart showing one example of authorizing an action;

Figure 3 is a flow chart showing an example embodiment of authorizing an action according to the present invention;

Figure 4 shows an alternative way of communicating between the token and the token issuer according to an example embodiment of the present invention;

Figure 5 is an alternative way of communicating between the control point and the control point issuer according to an example embodiment of the present invention; and

Figure 6 is a mobile communication device according to an example embodiment of the present invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

The present invention relates to authentication of an action between a user (e.g., a purchaser) and a control point (e.g., a device operated by a merchant) as will be described below. This may include such activities as payment at a point of sale (POS), authentication at an ATM machine, access control (e.g., doors), ticketing, toll collection and other similar types of actions. Embodiments of the present invention allow a user to authenticate an entity (hereafter referred to as a control point) on-line with the aid of supporting infrastructure. For example, an authenticating device (hereafter referred to as a token) may communicate with its own supporting and trusted infrastructure to perform the authentication. The infrastructure may help authenticate the control point for the user and authorize the action. By allowing for such verification, the user may make sure that to the best knowledge of the token issuer, the control point is valid and the interaction is secure. This may effectively disable fraudulent control points as each point can be verified by the user based on the trusted infrastructure. Interactions between the user and the control point

may be verified and authorized not only from the control point side but also from the user side as well.

Figure 1 shows entities involved in an example action such as a financial transaction. Other entities (not shown) may also be involved. Figure 1 shows a token issuer 10 that issues a token 50 to a user 20 (such as a purchaser). Figure 1 specifically shows the user 20 in possession of the token 50. The token issuer 10 may be a bank, credit union, security agency, etc. that is responsible for issuing tokens that will be presented to entities (i.e., control points) in order to perform an action. The token issuer 10 may be associated with a database of issued tokens 15 to store information and data about the tokens and users. Figure 1 also shows a control point operator 30 that approves control points such as a control point 40. The control point operator 30 may also be associated with a database of approved control points 35 to store information and data about the control points. The control point 40 may be any device or entity that is approved by the control point operator 30 to authenticate the user. The control point 40 may be operated by a merchant. The control point operator 30 may be an entity such as a bank, credit union or security agency that approves control points and provides means to authenticate the users and tokens. The token 50 may be a device that allows the user 20 to authenticate himself to the control point 40. Further, the user 20 may be a person or entity that has been granted the token 50 by the token issuer 10 and is authorized to use the token 50 at the control point 40.

Figure 2 shows one example of how a control point may authenticate a user. This figure will be described with respect to the entities that are shown in Figure 1. As shown in Figure 2, the token issuer 10 issues the token 50 in block 100. The token 50 is provided

to the user 20 in block 102. The token issuer 10 may store data about the token 50 in the database of the issued tokens 15 in block 104. The control point operator 30 may approve the control point 40 in block 106 and subsequently store data about the control point 40 in the database of approved control points 35 in block 108. In order to perform a particular action, the user 20 may present the token 50 to the control point 40 in block 110. The control point 40 may collect data (i.e., identification number or mother's maiden name) from the token 50 in block 112. The control point 40 may also interact with the control point operator 30 to authenticate the user 20 in block 114. The authentication may involve reviewing and comparing data from the token 50 with data stored in one of the databases 15, 35. If the control point operator 30 or the control point 40 authenticates the token 50, then the control point 40 may proceed with the respective action in block 116. Otherwise, the control point 40 may deny the action. In order to authenticate the tokens as being legitimate, the token issuer 10 may make the database of issued tokens 15 available to the control point operator 30.

Figure 3 shows a flow chart of an authenticating method according to an example embodiment of the present invention. This flow chart is merely one example embodiment as other embodiments are also within the scope of the present invention. Further, the order of the respective blocks of Figure 3 is merely illustrative as the order of the operations may differ in accordance with the present invention. The Figure 3 flow chart will be described with respect to the entities that are shown in Figure 1.

The token issuer 10 may issue the token 50 in block 100 and provide the token 50 to the user 20 in block 102. The token issuer 10 may store data (e.g., identification numbers or mother's maiden name) about the token 50 in the database of issued tokens 15 in block

104. The control point operator 30 may approve the control point 40 in block 106 and store data about the control point 40 in the database of approved control points 35 in block 108. In accordance with the present invention, the operations in blocks 106 and 108 may occur before, during or after the operations in blocks 100, 102 and 104.

5 The user 20 may present the token 50 to the control point 40 in block 110. The control point 40 may collect data from the token 50 in block 120. The token 50 or its underlying structure may also collect data from the control point 40 in block 120. The collected data may be any type of data that may be used to authenticate another entity. The control point 40 may interact with the control point operator 40 to authorize the user (and token) in block 122. The token 50 may interact with the token issuer 10 to authenticate the control point 40 in block 124. This authentication may occur on-line between the token 50 and the token issuer 10. The token 50 or its underlying structure may utilize the collected data regarding the control point 40 to determine if the control point 40 is a proper or legitimate entity. If the token 50 authenticates the control point 40 and if the control point 40 authenticates the token 50, then the transaction or action may properly proceed in block 126. If both the authentications do not occur, then the action or transaction may be denied.

10 In accordance with the present invention, the order of the control point collecting data from the token and the token collecting data from the control point may be different than that shown in Figure 3. Further, the order of the control point authorizing the token and the token authorizing the control point may be different than that shown in Figure 3. That is, other orders of these operations are also within the scope of the present invention.

20 The token 50 may be of different forms as will be described below. The token 50 or the structure to which it is attached may include electronic equipment to communicate

with both the user 20 and the token issuer 10. In order for the token issuer 10 to authenticate the control point 40, the database of approved control points 35 is made available for the token issuer 10. That is, the token issuer 10 may obtain information regarding the control point 40 from the database 35. Communication may occur between the token issuer 10 and the control point operator 30 in order to exchange the contents of the database of issued tokens 15 and the database of approved control points 35. The token 50 or the structure to which it is attached may interact with the token issuer infrastructure, such as the token issuer 10, so that the data collected by the token 50 from the control point 40 can be authenticated on-line using data from the database of approved control points 35.

Communication and exchange of data between the token 50 and the control point 40 may be conducted by several different types of methods including but not limited to local communication (e.g. Bluetooth) or remote communication such as the Internet. The token 50 may employ the necessary communication equipment to access the token issuer infrastructure by using GPRS or other types of wireless networks.

In one example embodiment, the control point 40 may communicate with the control point operator 30 across a normal communications link or direct connection. The token 50 may communicate with token issuer 10 using a wireless communication network or a direct connection. Further, the token issuer 10 may communicate with the control point operator 30 across a normal communications link or direct connection.

Figure 4 shows an embodiment in which the token 50 may use the communications network of the control point 40 in order to communicate on-line with the token user 10. That is, the token 50 may communicate with the token issuer 10 by using the same communication network that the control point 40 uses to communicate with the control

point operator 30. In such circumstances, the token 50 should establish a secure and reliable communication channel through the possibly hostile network of the control point 40.

Figure 5 shows an embodiment in which the control point 40 may use the communications network of the token 50 and the token issuer 10 in order to communicate with the control point operator 30. That is, the control point 40 may communicate with the control point operator 30 using the same communication network that the token 50 uses to communicate with the token issuer 10.

Figure 6 shows one embodiment of a token in which the token 50 is a mobile communication device 200. The token 50 may also be a part of the mobile communication device. The mobile communication device 200 may include a display device 210 and a data entry portion 220 such as a keypad. The mobile communication device 200 may further include a communication portion 230 and a portion 240 which is fitted within the mobile communication device 200 and adapted to receive a smart card or similar type of device containing data. The display device 210 may visually display information such as whether the control point is authenticated or denied. The mobile communication device 200 may also include a speaker (not shown) to make an audible sound authorizing or denying the control point 40. The communication device 230 may communicate over a wireless network with the token issuer 10 or may be connected by a direct communications link to the token issuer 10. The communication device 230 may be coupled by a direct communications link with the control point 40. The smart card may include data of the token 50 or user that will be used by the control point 40 for its authentication.

The token 50 may be a self-contained device that holds all the necessary interfaces such as the mobile communication device 200 shown in Figure 6 fitted with local communication circuits and with a tamper-proof circuit to hold the token's data. The token 50 may also be a self-contained device such as a smart card that provides only local communication (e.g., galvanic contact or contactless) and a user interface such as a display device and/or a keypad. The means in which the communication device 200 is connected and communicates with the control point 40 may be different than the means used to connect and communicate with the token issuer 10. The token 50 may also be separated from a communication device and connected to it when necessary. A smart card acting as a token may also be fitted into a mobile communication device or similar type of device. Alternatively, the token 50 may be a separate device that is coupled to the communication device (e.g., by contactless interface or Bluetooth).

Further, the token 50 may be fitted with communication facilities that can be used by the control point. Such a configuration may allow for authentication at passive control points such as door locks. The control point 40 may then establish the reliable communication with its operator and the control point may securely communicate the result of the authentication.

In accordance with the present invention, the user may be able to receive information regarding the authenticity or other characteristics of the control point. The token may be equipped with a user interface and the supporting infrastructure should be in place.

While the invention has been described with reference to specific embodiments, the description of the specific embodiments is illustrative only and is not to be considered as

limiting the scope of the invention. Various other modifications and changes may occur to those skilled in the art without departing from the spirit and scope of the invention.

WHAT IS CLAIMED IS:

1. A method of authenticating an action between a control point and a user, said method comprising:
presenting a token to said control point; and
authenticating said control point using said token.

2. The method of claim 1, said method further comprising a token issuer issuing said token to said user, and wherein said authenticating occurs on-line between said token and said token issuer.

3. The method of claim 2, wherein said token comprises a mobile communication device.

4. The method of claim 3, wherein said mobile communication device communicates with said token issuer using a wireless communication path.

5. The method of claim 2, wherein said token communicates with said token issuer using a communication network of said control point.

6. The method of claim 1, further comprising said control point authorizing said action based on information provided by said token.

- 1 7. The method of claim 1, wherein said action comprises a financial transaction.
- 1 8. The method of claim 1, wherein said action comprises access control.
- 1 9. The method of claim 1, wherein said authenticating comprises notifying said user
2 whether said control point has authorization for said action.
- 1 10. A method of authenticating a control point, said method comprising:
2 obtaining information regarding said control point; and
3 authenticating said control point based on said information.
- 1 11. The method of claim 10, wherein said information is obtained by presenting a token
2 to said control point.
- 1 12. The method of claim 11, said method further comprising a token issuer issuing a
2 token, and wherein said authenticating occurs on-line between said token and said token
3 issuer.
- 1 13. The method of claim 12, wherein said token comprises a mobile communication
2 device.
- 1 14. The method of claim 13, wherein said mobile communication device communicates
2 with said token issuer using a wireless communication path.

- 1 15. The method of claim 12, wherein said token communicates with said token issuer
2 using a communication network of said control point.
- 1 16. The method of claim 10, further comprising said control point authorizing an action
2 based on information provided by said token.
- 1 17. The method of claim 16, wherein said action comprises a financial transaction.
- 1 18. The method of claim 16, wherein said action comprises access control.
- 1 19. The method of claim 10, wherein said authenticating comprises notifying a user
2 whether said control point has authorization for said action.
- 3 20. A method of authenticating an action comprising:
4 presenting a token to said control point;
5 said control point collecting information from said token; and
6 authenticating said token based on said information.
- 1 21. The method of claim 20 further comprising a control point operator approving said
2 control point and said method further comprises storing data about said control point in a
3 database, and said authorizing comprises comparing said data with said information from
4 said token.

22. The method of claim 20, further comprising storing data about said token in a database, and said authorizing comprises comparing said data and said information from said token.

23. A token for authenticating a control point comprising:
a communication portion that obtains information regarding said control point and communicates with an external entity to authenticate said control point based on said information; and
a user interface portion coupled to said communication portion to indicate a result of said authentication to a user.

24. The token of claim 23, wherein said communication portion authenticates said control point on-line between said token and a token issuer that issued said token.

25. The token of claim 23, wherein said token comprises a mobile communication device.

26. The token of claim 23, wherein said communication portion authenticates said control point using a communication network of said control point.

27. The token of claim 23, wherein said action comprises a financial transaction.

28. The token of claim 23, wherein said action comprises access control.

1 29. The token of claim 23, wherein said user interface portion notifies said user whether
2 said control point has authorization for said action.

1 30. The token of claim 23, wherein said user interface portion comprises a display
2 device.

1 31. The token of claim 23, further comprising a card that connects with said
2 communication portion, said card containing information regarding one of said token and
3 said user.

1 32. The token of claim 23, wherein said communication portion is temporarily coupled
2 to said token.

ABSTRACT OF THE DISCLOSURE

A method is provided for authenticating an action between a control point and a user. A token is presented to the control point. The control point may be authenticated by using the token. The token may include a communication portion that obtains information regarding the control point and that communicates with a token issuer to authenticate the control point based on the information. A user interface portion may be coupled to the communication portion to indicate a result of the authentication to a user.

017.38726X00
NC29782

UNITED STATES PATENT APPLICATION FOR:

**METHOD AND TOKEN FOR AUTHENTICATING A
CONTROL POINT**

Inventor:

PIOTR COFTA

Prepared by:

Antonelli, Terry, Stout & Kraus, LLP
1300 North Seventeenth Street, Suite 1800
Arlington, Virginia 22209
Tel: 703/312-6600
Fax: 703/312-6666

METHOD AND TOKEN FOR AUTHENTICATING A CONTROL POINT

FIELD OF THE INVENTION

The present invention generally relates to a method and apparatus for authenticating an action. More particularly, the present invention relates to a method and token for authenticating a control point in a transaction or action.

DESCRIPTION OF RELATED ART

Financial transaction such as payment at a point of sale (POS) or the dispensing of monies at an ATM machine often include authorization of the user or purchaser by the entity providing the service, payment or object desired. The user or purchaser must often present identification for the authentication such as a card (e.g. a credit card or debit card) or a badge in order for the entity to authorize a particular action. The entity (e.g., merchant) may then verify the identity of the user through information that is then conveyed by the card, badge or other structure presented by the user. For example, a purchaser may provide a credit or debit card to a merchant who runs it through a card scanner to read out financial identification (ID) associated with the card. The financial ID and the cost of the goods or services may be forwarded over a telephone network (such as the public switched telephone network) to the bank or other entity providing the credit for the credit card or maintaining the money associated with the debit card. The bank verifies that there is

sufficient credit or debt capacity for the transaction and forwards verification to the merchant. The consumer then is typically asked to sign a receipt for the purchase and the transaction is thereby completed and the goods or services are conveyed to the consumer. However, in these transactions, the user or purchaser must trust the entity that he is presenting his identification card or badge. The entity to whom he presents his identification may be a fraudulent entity and may steal vital data or monies from the user.

Under current methods, the user or purchaser is unable to verify the authenticity of the entity other than observing the brand name, label or name of the entity. Any uncommon occurrence such as a malfunction at the entity makes the user feel uncomfortable.

Secure electronic transactions (SET) have recently been used for secure credit card payments over the Internet. In a remote payment SET, both the purchaser and the merchant may entrust the same organization to perform an off-line verification process. This off-line verification process may be in the form of cryptographic data exchange between the purchaser and the merchant. However, secure electronic transactions do not address other aspects of the payment and assume that the purchaser is satisfied with the off-line authentication of the digital certificate that is presented by the merchant. It is desirable to obtain further authentication of merchants.

SUMMARY OF THE INVENTION

A method is provided for authenticating (or verifying) an action (e.g. financial action, access control, ticketing, and toll collecting) between a control point and a user.

The method may involve presenting a token to the control point and authenticating the control point using the token.

The authentication may occur on-line between the token and a token issuer that issued the token to the user.

5 The token may be a mobile communication device that communicates with the token issuer using a wireless communication path. The token may also communicate with the token issuer using a communication network of the control point. The control point may also authorize the action based on information provided by the token.

10 A token may be provided for authenticating a control point. The token may include a communication portion that obtains information regarding the control point and that communicates with an external entity (e.g., a token issuer) to authenticate the control point based on the information. A user interface portion may be coupled to the communication portion to indicate a result of the authentication to a user.

15 Other objects, advantages and salient features of the invention will become apparent from the following detailed description taken in conjunction with the annexed drawings, which disclose preferred embodiments of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention will be described with reference to the following drawings in which like reference numerals refer to like elements and wherein:

20 Figure 1 is a block diagram of entities involved in a financial transaction;

Figure 2 is a flow chart showing one example of authorizing an action;

Figure 3 is a flow chart showing an example embodiment of authorizing an action according to the present invention;

Figure 4 shows an alternative way of communicating between the token and the token issuer according to an example embodiment of the present invention;

Figure 5 is an alternative way of communicating between the control point and the control point issuer according to an example embodiment of the present invention; and

Figure 6 is a mobile communication device according to an example embodiment of the present invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

The present invention relates to authentication of an action between a user (e.g., a purchaser) and a control point (e.g., a device operated by a merchant) as will be described below. This may include such activities as payment at a point of sale (POS), authentication at an ATM machine, access control (e.g., doors), ticketing, toll collection and other similar types of actions. Embodiments of the present invention allow a user to authenticate an entity (hereafter referred to as a control point) on-line with the aid of supporting infrastructure. For example, an authenticating device (hereafter referred to as a token) may communicate with its own supporting and trusted infrastructure to perform the authentication. The infrastructure may help authenticate the control point for the user and authorize the action. By allowing for such verification, the user may make sure that to the best knowledge of the token issuer, the control point is valid and the interaction is secure. This may effectively disable fraudulent control points as each point can be verified by the user based on the trusted infrastructure. Interactions between the user and the control point

may be verified and authorized not only from the control point side but also from the user side as well.

Figure 1 shows entities involved in an example action such as a financial transaction. Other entities (not shown) may also be involved. Figure 1 shows a token issuer 10 that issues a token 50 to a user 20 (such as a purchaser). Figure 1 specifically shows the user 20 in possession of the token 50. The token issuer 10 may be a bank, credit union, security agency, etc. that is responsible for issuing tokens that will be presented to entities (i.e., control points) in order to perform an action. The token issuer 10 may be associated with a database of issued tokens 15 to store information and data about the tokens and users. Figure 1 also shows a control point operator 30 that approves control points such as a control point 40. The control point operator 30 may also be associated with a database of approved control points 35 to store information and data about the control points. The control point 40 may be any device or entity that is approved by the control point operator 30 to authenticate the user. The control point 40 may be operated by a merchant. The control point operator 30 may be an entity such as a bank, credit union or security agency that approves control points and provides means to authenticate the users and tokens. The token 50 may be a device that allows the user 20 to authenticate himself to the control point 40. Further, the user 20 may be a person or entity that has been granted the token 50 by the token issuer 10 and is authorized to use the token 50 at the control point 40.

Figure 2 shows one example of how a control point may authenticate a user. This figure will be described with respect to the entities that are shown in Figure 1. As shown in Figure 2, the token issuer 10 issues the token 50 in block 100. The token 50 is provided

to the user 20 in block 102. The token issuer 10 may store data about the token 50 in the database of the issued tokens 15 in block 104. The control point operator 30 may approve the control point 40 in block 106 and subsequently store data about the control point 40 in the database of approved control points 35 in block 108. In order to perform a particular
5 action, the user 20 may present the token 50 to the control point 40 in block 110. The control point 40 may collect data (i.e., identification number or mother's maiden name) from the token 50 in block 112. The control point 40 may also interact with the control point operator 30 to authenticate the user 20 in block 114. The authentication may involve reviewing and comparing data from the token 50 with data stored in one of the databases
10 15, 35. If the control point operator 30 or the control point 40 authenticates the token 50, then the control point 40 may proceed with the respective action in block 116. Otherwise, the control point 40 may deny the action. In order to authenticate the tokens as being legitimate, the token issuer 10 may make the database of issued tokens 15 available to the control point operator 30.

Figure 3 shows a flow chart of an authenticating method according to an example
15 embodiment of the present invention. This flow chart is merely one example embodiment as other embodiments are also within the scope of the present invention. Further, the order of the respective blocks of Figure 3 is merely illustrative as the order of the operations may differ in accordance with the present invention. The Figure 3 flow chart will be described
20 with respect to the entities that are shown in Figure 1.

The token issuer 10 may issue the token 50 in block 100 and provide the token 50 to the user 20 in block 102. The token issuer 10 may store data (e.g., identification numbers or mother's maiden name) about the token 50 in the database of issued tokens 15 in block

104. The control point operator 30 may approve the control point 40 in block 106 and store data about the control point 40 in the database of approved control points 35 in block 108. In accordance with the present invention, the operations in blocks 106 and 108 may occur before, during or after the operations in blocks 100, 102 and 104.

5 The user 20 may present the token 50 to the control point 40 in block 110. The control point 40 may collect data from the token 50 in block 120. The token 50 or its underlying structure may also collect data from the control point 40 in block 120. The collected data may be any type of data that may be used to authenticate another entity. The control point 40 may interact with the control point operator 40 to authorize the user (and token) in block 122. The token 50 may interact with the token issuer 10 to authenticate the control point 40 in block 124. This authentication may occur on-line between the token 50 and the token issuer 10. The token 50 or its underlying structure may utilize the collected data regarding the control point 40 to determine if the control point 40 is a proper or legitimate entity. If the token 50 authenticates the control point 40 and if the control point 40 authenticates the token 50, then the transaction or action may properly proceed in block 126. If both the authentications do not occur, then the action or transaction may be denied.

10 In accordance with the present invention, the order of the control point collecting data from the token and the token collecting data from the control point may be different than that shown in Figure 3. Further, the order of the control point authorizing the token and the token authorizing the control point may be different than that shown in Figure 3. That is, other orders of these operations are also within the scope of the present invention.

20 The token 50 may be of different forms as will be described below. The token 50 or the structure to which it is attached may include electronic equipment to communicate

with both the user 20 and the token issuer 10. In order for the token issuer 10 to authenticate the control point 40, the database of approved control points 35 is made available for the token issuer 10. That is, the token issuer 10 may obtain information regarding the control point 40 from the database 35. Communication may occur between the token issuer 10 and the control point operator 30 in order to exchange the contents of the database of issued tokens 15 and the database of approved control points 35. The token 50 or the structure to which it is attached may interact with the token issuer infrastructure, such as the token issuer 10, so that the data collected by the token 50 from the control point 40 can be authenticated on-line using data from the database of approved control points 35.

Communication and exchange of data between the token 50 and the control point 40 may be conducted by several different types of methods including but not limited to local communication (e.g. Bluetooth) or remote communication such as the Internet. The token 50 may employ the necessary communication equipment to access the token issuer infrastructure by using GPRS or other types of wireless networks.

In one example embodiment, the control point 40 may communicate with the control point operator 30 across a normal communications link or direct connection. The token 50 may communicate with token issuer 10 using a wireless communication network or a direct connection. Further, the token issuer 10 may communicate with the control point operator 30 across a normal communications link or direct connection.

Figure 4 shows an embodiment in which the token 50 may use the communications network of the control point 40 in order to communicate on-line with the token user 10. That is, the token 50 may communicate with the token issuer 10 by using the same communication network that the control point 40 uses to communicate with the control

point operator 30. In such circumstances, the token 50 should establish a secure and reliable communication channel through the possibly hostile network of the control point 40.

Figure 5 shows an embodiment in which the control point 40 may use the communications network of the token 50 and the token issuer 10 in order to communicate with the control point operator 30. That is, the control point 40 may communicate with the control point operator 30 using the same communication network that the token 50 uses to communicate with the token issuer 10.

Figure 6 shows one embodiment of a token in which the token 50 is a mobile communication device 200. The token 50 may also be a part of the mobile communication device. The mobile communication device 200 may include a display device 210 and a data entry portion 220 such as a keypad. The mobile communication device 200 may further include a communication portion 230 and a portion 240 which is fitted within the mobile communication device 200 and adapted to receive a smart card or similar type of device containing data. The display device 210 may visually display information such as whether the control point is authenticated or denied. The mobile communication device 200 may also include a speaker (not shown) to make an audible sound authorizing or denying the control point 40. The communication device 230 may communicate over a wireless network with the token issuer 10 or may be connected by a direct communications link to the token issuer 10. The communication device 230 may be coupled by a direct communications link with the control point 40. The smart card may include data of the token 50 or user that will be used by the control point 40 for its authentication.

The token 50 may be a self-contained device that holds all the necessary interfaces such as the mobile communication device 200 shown in Figure 6 fitted with local communication circuits and with a tamper-proof circuit to hold the token's data. The token 50 may also be a self-contained device such as a smart card that provides only local communication (e.g., galvanic contact or contactless) and a user interface such as a display device and/or a keypad. The means in which the communication device 200 is connected and communicates with the control point 40 may be different than the means used to connect and communicate with the token issuer 10. The token 50 may also be separated from a communication device and connected to it when necessary. A smart card acting as a token may also be fitted into a mobile communication device or similar type of device. Alternatively, the token 50 may be a separate device that is coupled to the communication device (e.g., by contactless interface or Bluetooth).

Further, the token 50 may be fitted with communication facilities that can be used by the control point. Such a configuration may allow for authentication at passive control points such as door locks. The control point 40 may then establish the reliable communication with its operator and the control point may securely communicate the result of the authentication.

In accordance with the present invention, the user may be able to receive information regarding the authenticity or other characteristics of the control point. The token may be equipped with a user interface and the supporting infrastructure should be in place.

While the invention has been described with reference to specific embodiments, the description of the specific embodiments is illustrative only and is not to be considered as

limiting the scope of the invention. Various other modifications and changes may occur to those skilled in the art without departing from the spirit and scope of the invention.

WHAT IS CLAIMED IS:

1. A method of authenticating an action between a control point and a user, said method comprising:
presenting a token to said control point; and
authenticating said control point using said token.

2. The method of claim 1, said method further comprising a token issuer issuing said token to said user, and wherein said authenticating occurs on-line between said token and said token issuer.

3. The method of claim 2, wherein said token comprises a mobile communication device.

4. The method of claim 3, wherein said mobile communication device communicates with said token issuer using a wireless communication path.

5. The method of claim 2, wherein said token communicates with said token issuer using a communication network of said control point.

6. The method of claim 1, further comprising said control point authorizing said action based on information provided by said token.

1 7. The method of claim 1, wherein said action comprises a financial transaction.

1 8. The method of claim 1, wherein said action comprises access control.

1 9. The method of claim 1, wherein said authenticating comprises notifying said user
2 whether said control point has authorization for said action.

1 10. A method of authenticating a control point, said method comprising:
2 obtaining information regarding said control point; and
3 authenticating said control point based on said information.

1 11. The method of claim 10, wherein said information is obtained by presenting a token
2 to said control point.

1 12. The method of claim 11, said method further comprising a token issuer issuing a
2 token, and wherein said authenticating occurs on-line between said token and said token
3 issuer.

1 13. The method of claim 12, wherein said token comprises a mobile communication
2 device.

1 14. The method of claim 13, wherein said mobile communication device communicates
2 with said token issuer using a wireless communication path.

1 15. The method of claim 12, wherein said token communicates with said token issuer
2 using a communication network of said control point.

1 16. The method of claim 10, further comprising said control point authorizing an action
2 based on information provided by said token.

1 17. The method of claim 16, wherein said action comprises a financial transaction.

1 18. The method of claim 16, wherein said action comprises access control.

1 19. The method of claim 10, wherein said authenticating comprises notifying a user
2 whether said control point has authorization for said action.

1 20. A method of authenticating an action comprising:
2 presenting a token to said control point;
3 said control point collecting information from said token; and
4 authenticating said token based on said information.

1 21. The method of claim 20 further comprising a control point operator approving said
2 control point and said method further comprises storing data about said control point in a
3 database, and said authorizing comprises comparing said data with said information from
4 said token.

22. The method of claim 20, further comprising storing data about said token in a database, and said authorizing comprises comparing said data and said information from said token.

23. A token for authenticating a control point comprising:
a communication portion that obtains information regarding said control point and communicates with an external entity to authenticate said control point based on said information; and
a user interface portion coupled to said communication portion to indicate a result of said authentication to a user.

24. The token of claim 23, wherein said communication portion authenticates said control point on-line between said token and a token issuer that issued said token.

25. The token of claim 23, wherein said token comprises a mobile communication device.

26. The token of claim 23, wherein said communication portion authenticates said control point using a communication network of said control point.

27. The token of claim 23, wherein said action comprises a financial transaction.

28. The token of claim 23, wherein said action comprises access control.

1 29. The token of claim 23, wherein said user interface portion notifies said user whether
2 said control point has authorization for said action.

1 30. The token of claim 23, wherein said user interface portion comprises a display
2 device.

1 31. The token of claim 23, further comprising a card that connects with said
2 communication portion, said card containing information regarding one of said token and
said user.

1 32. The token of claim 23, wherein said communication portion is temporarily coupled
2 to said token.

ABSTRACT OF THE DISCLOSURE

A method is provided for authenticating an action between a control point and a user. A token is presented to the control point. The control point may be authenticated by using the token. The token may include a communication portion that obtains information regarding the control point and that communicates with a token issuer to authenticate the control point based on the information. A user interface portion may be coupled to the communication portion to indicate a result of the authentication to a user.

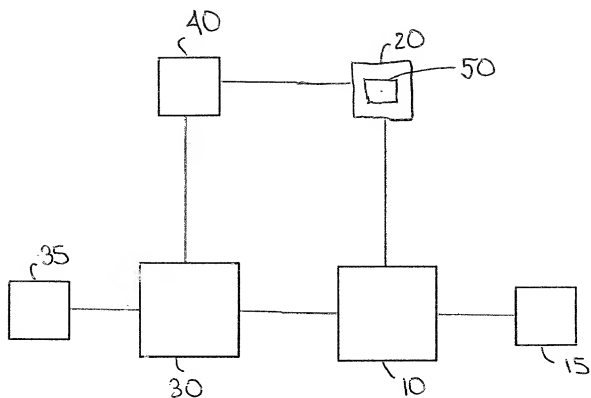


FIG. 1

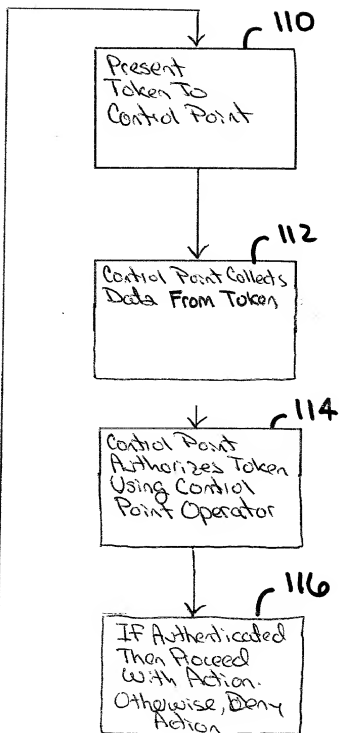
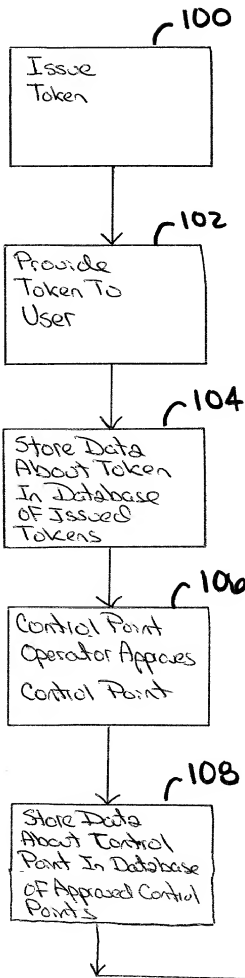


FIG. 2

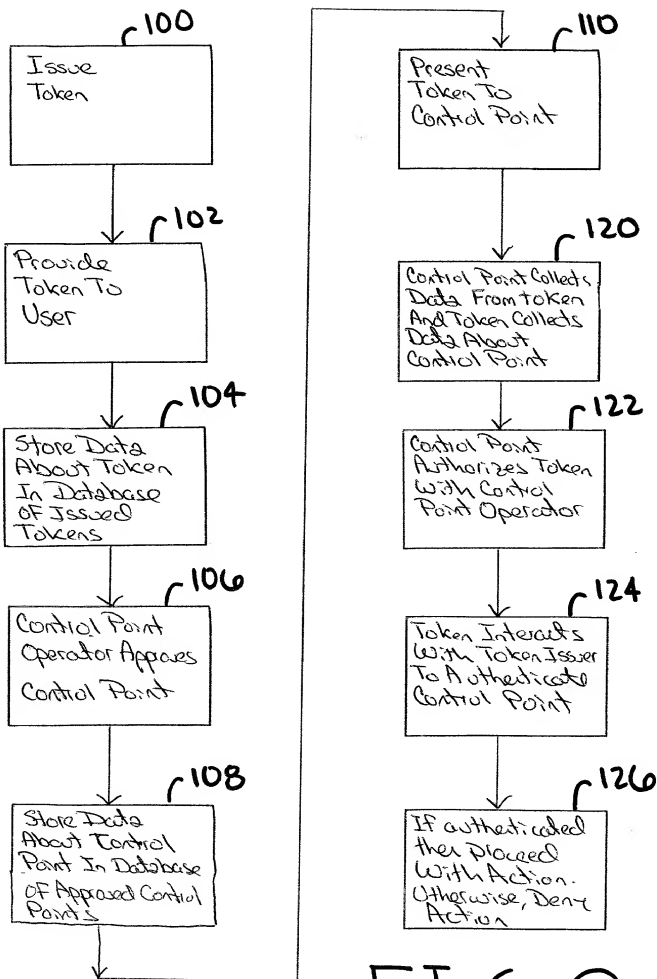


FIG. 3

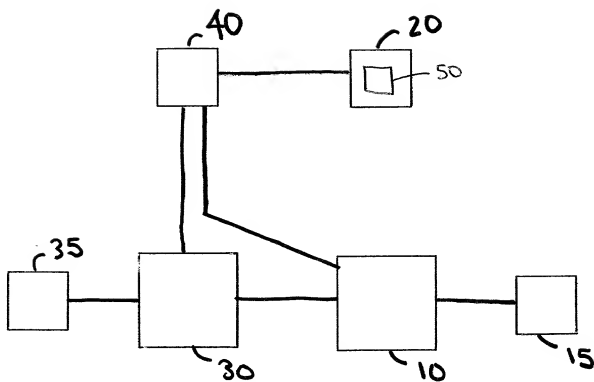


FIG. 4

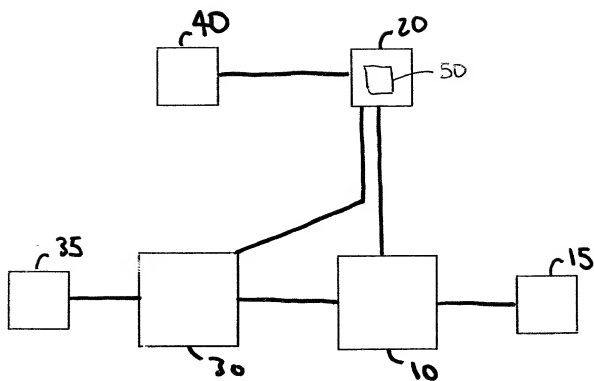


FIG. 5

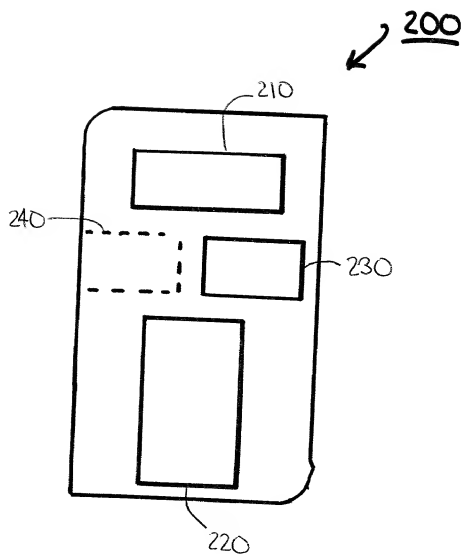


FIG. 6

DECLARATION AND POWER OF ATTORNEY - PATENT APPLICATION

As a below named inventor, I hereby declare: that my citizenship, residence and post office address are as stated below; that I verily believe I am the original, first and sole inventor (if only one is named below) or a joint inventor (if plural inventors are named below) of the invention entitled: METHOD AND TOKEN FOR AUTHENTICATING A CONTROL POINT

the specification of which X is attached hereto

— was filed on _____ as Application
Serial No. _____ and was amended on
_____.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above. I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56(a). I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)

Priority Claimed

(Number)

(Country)

(Day/Month/Year Filed)

Yes

No

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application;

(Application Serial No.)

(Filing Date)

(Status-patented, pending
or abandoned.)

I hereby appoint as principal attorneys: Donald R. Antonelli, Reg. No. 20,296; David T. Terry, Reg. No. 20,178; Melvin Kraus, Reg. No. 22,466; William I. Solomon, Reg. No. 28,565; Gregory E. Montone, Reg. No. 28,141; Ronald J. Shore, Reg. No. 28,577; Donald E. Stout, Reg. No. 26,422; Alan E. Schiavelli, Reg. No. 32,087; James N. Dresser, Reg. No. 22,973; Carl I. Brundidge, Reg. No. 29,621; and Paul J. Skwierawski, Reg. No. 32,173; to prosecute and transact all business in the Patent and Trademark Office connected with this

application and any related United States and international applications.

Please Direct all Communications to:

Direct Telephone Calls To:

Antonelli, Terry, Stout & Kraus, LLP
Suite 1800
1300 North Seventeenth Street
Arlington, Virginia 22209

(703) 312-6600

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

(Full Name)

(Signature)

PIOTR COFTA



Date 08/25/00 Inventor Piotr Cofta

Residence Arlington, MA Citizenship Polish

Post Office Address 35 Milton Street, Arlington, MA 02474